Army Information Technology Registry (AITR) Instruction Manual

The AITR is the Army's single, definitive registry of IT systems. The AITR provides data on:

- the inventory of Army systems/applications
- current status of webification
- system milestones for reduction/webification
- tracking of Federal Information Security Management Act (FISMA) data
- Privacy Impact Assessment (PIA) data [planned for early 2004]

In addition, it is used to support IM/IT resource management, business/functional process improvement efforts, provide input to the Strategic Readiness System (SRS), and for compiling information for FISMA status reports to OMB and Congress. PIA fields will also be included because they are required by the provisions in OMB Memorandum "Guidance for Implementing the Privacy Provision of the E-Government Act of 2002, dated September 26, 2003

This documents the steps associated with adding, deleting and editing systems with the AITR. The document includes the following sections:

1. **TO ADD A NEW SYSTEM:** Systems should be added to AITR if they meet the definition of a system, are owned by your organization, and are not already in AITR. To add a new system, send an e-mail containing the information identified in Table 1 to your MACOM POC. The MACOM POC will review your request and if approved will create a record in AITR. Prior to adding new systems, they will query AITR to determine whether the proposed system is already in AITR. Table 1 contains a description of all the fields associated with an AITR record, the fields represented by an asterisk must be identified before a system can be entered into the AITR database.

Table 1: Table of AITR Fields – Mandatory entry fields are marked by asterisk

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
SYSTEM ID	NA	The System ID field is a system generated field that serves as the unique identifier of an AITR record. Format is DAnnnnn.

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
DOD Registration ID	NA	The DoD Registration ID field is a unique identifier of Mission Critical (MC) or Mission Essential (ME) systems. This number is assigned by CIO/G6 after a Functional Proponent certifies a system as MC or ME. Format is ABnnnnnn.
MISSION_CRITICAL	NA	The Mission Critical field identifies the mission criticality of this IT system. All records are initially created with a status of "Other." See Section 2 for changing mission criticality to have status raised to MC or ME.
MAC_CATEGORY	NA	The Mission Assurance Category field identifies the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. This will become a mandatory field. Acceptable values: **MAC I, MAC II, MAC III, or NA.**
MACOM/DA Staff Owner	NA	The MACOM/DA Staff Owner field provides the name of the organization that owns this system. This field is automatically set to the organization that creates the record. To change it, see Section 3 on transferring systems.
*SYSTEM_ACRONYM	30	The System Acronym field represents a shortened or commonly used name or abbreviation (upper case) for this IT System.
*SYSTEM_NAME	100	The System Name field is the full descriptive name for this IT system (upper case).
*BMMP Domain	NA	The Business Management Modernization Program (BMMP) domain field identifies the domain that best matches the function delivered by the IT system. Warfighting domain systems should be entered as "Other". Acceptable values: **Accounting and Finance; Acquisition/Procurement; Human Resources; Installations and Environment; Logistics; Strategic Planning and Budget; Technical Infrastructure; Other**. Further information about BMMP is available from: http://www.dod.mil/comptroller/bmmp/pages/index.html
*SYSTEM_DESCRIPT	1000	The System Description field is a free form text description of the system, its function, and uses.
*ACQ_CATEGORY	3	The Acquisition Category field represents the acquisition category for this program. Accept-

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
		able values: **ID, IC, IAM, IAC, II, III, IV, or NA**.
*FUNC_AREA	50	The Functional Area field relates to the functions under which this particular IT system is reported. For acceptable values, see **Table 2: Functional Areas Table** below.
SEC_FUNC_AREA	50	The Secondary Functional Area field is for use if this IT system has a secondary function. For acceptable values, see **Table 2: Functional Areas Table** below.
TERC_FUNC_AREA	50	The Tertiary Functional Area is for use if this IT system has a tertiary function. For acceptable values, see **Table 2: Functional Areas Table** below.
PM_NAME	50	The Project Manager field identifies the First and Last name of Program Manager (PM) or POC for this IT System
PM_TITLE	10	The PM Title field identifies the Rank, Grade, and Title of PM or POC or Systems Manager.
PM_ORGANIZATION	50	The PM Organization field identifies the Organization of PM or POC or Systems Manager.
PM_COM_PHONE	18	The PM Com Phone field identifies the Commercial phone number of PM or POC or Systems Manager.
PM_DSN_PHONE	18	The PM DSN Phone field identifies the Defense Switched Network phone number of PM or POC or Systems Manager.
PM_EMAIL	100	The PM Email field identifies the Email address of PM or POC or Systems Manager.
REC_TYPE	NA	The Record Type field identifies the type of entity represented by this particular IT Registry entry. Acceptable values are: **System, Application, Acquisition Program, Network, or Enclave**.
BIN	6	The Budget Initiative Number field contains the Budget Initiative Number if it exists, from the Information Technology Management Application (ITMA) Database.
INTERFACES_IDENTIFIED	3	The Interfaces Identified field indicates if the system interfaces between this IT system and other systems have all been identified. Acceptable values are **Yes, No, or NA**.
CONTINGENCY_PLAN	3	The Contingency Plan field indicates if a contingency plan is in place to account for disruptions in the operations of this system. Acceptable values are **Yes, No, or NA**.
LIFE_CYCLE	64	The Life Cycle field identifies the phase of the system life cycle this IT Registry entity is in.

<table>
<tr><th>FIELD NAME</th><th>FIELD SIZE</th><th>FIELD DESCRIPTION</th></tr>
<tr><td></td><td></td><td>Acceptable values are: Concept Refinement; MS - A Technology Development; MS – B System Development & Demonstration; MS – C Production & Deployment; Demonstration, Production & Deployment; Operations & Support; or Disposal.</td></tr>
<tr><td>Accreditation Required [ACCRED_REQUIRED]</td><td>3</td><td>The Accreditation Required field identifies whether this entry require completion of a Department of Defense approved Information Technology Security Certification and Accreditation Process. Acceptable values are: Yes, No.

If any questions, See DoDD 8500.1 Section 2.

Examples as they apply to Platform IT or Interconnection Components:

<table>
<tr><th>Platform IT or Interconnection Components</th><th>DoDD 8500.1 Applies</th></tr>
<tr><td>IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)</td><td>No</td></tr>
<tr><td>IT which is integral to real-time execution of the platform mission (e.g., sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)</td><td>No</td></tr>
<tr><td>IT that is part of or connected with the platform that also connects to external applications that process data in support of the platform (e.g., logistics, training, scheduling, remote diagnostics, etc.)</td><td>Yes</td></tr>
<tr><td>IT that is part of or connected with the platform that is part of a defined Information Exchange Requirement (IER) or interfaces with the GIG</td><td>Yes</td></tr>
</table>

If “No” is selected, a reason in the “ACCREDITATION DOES NOT APPLY EXPLANATION:” [NOTAPPLY_EXPLANATION] field is required. Additionally, the following fields do not need to be populated: ACCRED_STATUS, ACCRED_DATE,</td></tr>
</table>

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
		ACCRED_EXPIRATION, ACCRED_VEHICLE, ACCRED-DOC, SSAA_STATUS, ACCESS_CONTROL, ADMIN_CONTROL, LIFE_CYCLE_PLAN, LIFE_CYCLE_COSTS, MAINTENANCE_PLAN, RISK_PLAN, SECURITY_PLAN, CSIRT, SECURITY_CONTROL_TEST, VIRUS_PROTECTION, DAA_NAME, DAA_TITLE, DAA_ORG, DAA_PHONE, DAA_EMAIL.
ACCREDITATION DOES NOT APPLY EXPLANATION	50	The ACCREDITATION DOES NOT APPLY EXPLANATION field provides an explanation as to why this entry does not require a Certification and Accreditation during its lifecycle. Acceptable values: **Embedded IT, Integral to real-time execution, Without Platform Interconnection, or NA**. Select NA if ACCRED_REQUIRED is "Yes"
ACCRED_VEHICLE	10	The Accreditation Vehicle field identifies the certification and accreditation (C&A) process was used to grant the current certification and accreditation (C&A). Acceptable values: **DITSCAP, DIACAP, DCID 6/3, AFSSI 5024, AR 380-19, Other.**
ACCRED_STATUS	10	The Accreditation Vehicle field identifies whether your system has undergone a certification and accreditation process and if so, what its current status is. Acceptable values: **Final** – Authority to Operate; **IATO** – Interim Authority to Operate; **None** – Not Yet Accredited.
ACCRED_DATE	9 DDMMMYYYY	The Accreditation Date field identifies the date the current certification and accreditation (C&A) status was granted. Acceptable values are dates entered as day [**2** digits], month [**3** alpha], year [**4** digits] e.g. 05JAN2003. **If system has no accreditation, enter the projected accreditation dates. Future dates should result in the ACCRED_STATUS field set to "None."
ACCRED_EXPIRATION	9 DDMMMYYYY	The Accreditation Expiration Date field identifies the date the current certification and accreditation (C&A) is set to expire. Acceptable values are dates entered as day [**2** digits], month [**3** alpha], year [**4** digits] e.g. 05JAN2003. A Final Accreditation expiration date cannot exceed 3 years from the value in the ACCRED_DATE field An IATO Accreditation expiration date cannot exceed 1 year from the value in the ACCRED_DATE field

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
ACCRED_DOC	3	The Accreditation Documentation field identifies whether, if your system has a certification and accreditation (C&A), you have formal documentation that indicates the specifics of the certification and accreditation (C&A) process. Acceptable values: **Yes, No**.
SSAA_STATUS	4	The Systems Security Authorization Agreement (SSAA) Status field identifies which phase of the SSAA your system is in. Acceptable values: **I, II, III, IV, or None.** The phases of the SSAA are based on Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) definitions. See Section 6 Definitions below.
CONTINGENCY_TEST	9 DDMMMYYYY	The Contingency Plan/Continuity of Operations Plan (COOP) field identifies the last time that your system's contingency plan/COOP was exercised. Acceptable values are dates entered as day [**2** digits], month [**3** alpha], year [**4** digits] e.g. 05JAN2003
ACCESS_CONTROL	3	The Access Controls field identifies whether your system has measures in place that control access and prevent the circumvention of the security software and application controls. Acceptable values: **Yes, No.**
ADMIN_CONTROL	3	The Administrative Controls field identifies whether your system has measures in place that ensure the proper administration of your system to include identification of users, groups, and their privileges as well as the capability to produce system activity audit logs. Acceptable values: **Yes, No.**
LIFE_CYCLE_PLAN	3	The System Life Cycle Plan field identifies whether your system has a life cycle plan that discusses at minimum the basic life cycle phases. Acceptable values: **Yes, No.**
LIFE_CYCLE_COSTS	3	The Life Cycle Costs field identifies whether your system has the costs of its security controls in the life cycle documentation of the system. Acceptable values: **Yes, No.**
MAINTENANCE_PLAN	3	The Hardware/Software Maintenance Plan field identifies whether your system has controls that are used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Acceptable values: **Yes, No.**

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
RISK_PLAN	3	The Risk Management Plan field identifies whether your system has a risk management plan that identifies the risks and vulnerabilities to the system, recognizes the sensitivity of the data and lays out a plan to mitigate those risks and vulnerabilities. Acceptable values: **Yes, No.**
SECURITY_PLAN	3	The System Security Plan field identifies whether your system has a system security plan that provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. Does the plan delineate responsibilities and expected behavior of all individuals who access the system? Acceptable values: **Yes, No.**
CSIRT	3	The Computer Security Incident Response Team (CSIRT) field identifies whether your system has controls (e.g. Security Incident Response Team, etc.) in place to recognize, report, monitor and efficiently handle incidents, and if there is a capability to share this information with appropriate organizations. Acceptable values: **Yes, No.**
SECURITY_CONTROL_TEST	9 DDMMMYYYY	The Security Controls Tested field identifies the last date system security controls were tested. SSAA should document the initial and subsequent testing and validation. **FISMA requires evaluation annually.** DoDI 8500.2 controls provide additional basis for evaluation. **Management Controls** - Controls that address the security management aspects of the IT system and the management of risk for the system **Operational Controls** - Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems) **Technical Controls** - Controls that address security mechanisms contained in and executed by the computer system. Acceptable values are dates entered as day [**2** digits], month [**3** alpha], year [**4** digits] e.g. 05JAN2003.
VIRUS_PROTECTION	3	The Virus Protection field identifies whether your system has virus protection and data integrity controls that protect data from accidental or malicious alteration or destruction and that protect your system from infection from malicious computer viruses. Acceptable values: **Yes, No.**
DAA_NAME	50	The Designated Approving Authority (DAA)

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
		Name field identifies the name of the DAA who granted the system a certification and accreditation (C&A) status. Acceptable value: First and Last name.
DAA_TITLE	100	The Designated Approving Authority (DAA) Title field identifies the title of the DAA who granted the system a certification and accreditation (C&A) status. Acceptable value: **Title** up to 100 characters.
DAA_ORG	50	The Designated Approving Authority (DAA) Organization field identifies the organization of the DAA who granted the system a certification and accreditation (C&A) status. Acceptable value: **Organization** up to 50 characters.
DAA_PHONE	18	The Designated Approving Authority (DAA) phone field identifies the phone number of the DAA who granted the system a certification and accreditation (C&A) status. Acceptable value: **Phone number and Extension.**
DAA_EMAIL	100	The Designated Approving Authority (DAA) Email field identifies the e-mail address of the DAA who granted the system a certification and accreditation (C&A) status. Acceptable value: **Email address.**
PIA_ Requirement	3	The PIA Requirement field identifies whether or not a privacy impact assessment is required for a new or previously existing IT system based on the provisions in OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIB. http://www.whitehouse.gov/omb/memoranda/m03-22.html Acceptable values: **Yes, No.**
PIA_ Review	TBD	The PIA Review field identifies whether or not the PIA has been reviewed (by the Component Privacy Office and CIO) and approved in accordance with OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIC3ai. http://www.whitehouse.gov/omb/memoranda/m03-22.html Indicate "NA" only if a PIA is not required. If "No" is indicated, provide explanation. Acceptable values: **Yes, No, NA.**
PIA_ Public	TBD	The PIA Public Availability field identifies whether or not the PIA has been made available

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
		for public review in accordance with OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIC3aiii. www.whitehouse.gov/omb/memoranda/m03-22.html Indicate "NA" only if a PIA is not required. If "No" is indicated, provide explanation. Acceptable values: **Yes, No, NA.**
PIA_OMB	TBD	The PIA Submission to OMB field identifies whether or not a copy of the PIA has been provided to OMB in accordance with OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIC3aii. www.whitehouse.gov/omb/memoranda/m03-22.html Indicate "NA" only if a PIA is not required. If "No" is indicated, provide explanation. Acceptable values: **Yes, No, NA.**
Comments	255 and then 1000 when switched new DB	The Comments field is mandatory for any PIA answer that is No. Acceptable value: free text up to **255 characters** [will increase to 1000 during 2004].
WEB ENABLED PROJECTED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab as an initial plan if no plan exists. The MACOM/DA staff AITR administrator will review the date. If approved it will be reflected in AITR. To change projected dates see Section 2: "TO EDIT A SYSTEM RECORD"
WEB ENABLED COMPLETED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab. The MACOM/DA staff AITR administrator will review the date. If approved it will be reflected in AITR. To change completed dates see Section 2: "TO EDIT A SYSTEM RECORD"
AKO-LINKED PROJECTED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab as an initial plan if no plan exists. The MACOM/DA staff AITR administrator will review the date. If approved it will be reflected in AITR. To change projected dates see Section 2: "TO EDIT A SYSTEM RECORD"
AKO-LINKED COMPLETED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab. The MACOM/DA staff

FIELD NAME	FIELD SIZE	FIELD DESCRIPTION
		AITR administrator will review the date. If approved it will be reflected in AITR. To change completed dates see Section 2: "TO EDIT A SYSTEM RECORD"
AKO SINGLE SIGN-ON PROJECTED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab as an initial plan if no plan exists. The MACOM/DA staff AITR administrator will review the date. If approved it will be reflected in AITR. To change projected dates see Section 2: "TO EDIT A SYSTEM RECORD"
AKO SINGLE SIGN-ON COMPLETED DATE	8 MMDDYYYY	These values are entered through the AITR "Webification" tab. The MACOM/DA staff AITR administrator will review the date. If approved it will be reflected in AITR. To change completed dates see Section 2: "TO EDIT A SYSTEM RECORD"

Table 2: Acceptable Functional Areas

FUNCTIONAL AREAS
Allies
Chemical, Biological, Radiological, and Nuclear and High Yield Explosive (CBRNE)
Civilian Personnel & Readiness
Command and Control
Communications
Communications Security (COMSEC)
Economic
Environmental Security
Facilities
Finance
Health/Medical
Human Resources
Information Management
Inspector General
Intelligence
Legal
Logistics
Military Personnel and Readiness
Nuclear
Nuclear, Chemical, and Biological
Operations
Personnel and Readiness
Procurement/Acquisition
Reserve Components
Scientific and Engineering
Space and Weather
Test and Evaluation
Trainers
Transportation
Weapons
Not Applicable (NA)

2. **TO EDIT SYSTEM INFORMATION:** Points of Contacts (POCs) can edit basic application information. Changes to webification dates or to address webification exemptions must be worked with CIO/G6 through individual MACOM/DA AITR Administrators.

   a. **TO EDIT BASIC APPLICATION INFORMATION.** The system Point of Contact can directly edit the fields identified in Table 3 for those AITR records assigned to them.

Table 3: POC Editable Application Fields

APPLICATION FIELDS
System Name
System Acronym

APPLICATION FIELDS
System Description
Acquisition Category
Functional Area
Secondary Functional Area
Tertiary Functional Area
Project Manager
PM Title
PM Organization
PM Com Phone
PM DSN Phone
PM Email
Budget Initiative Number
Interfaces Identified
Contingency Plan

b. **TO EDIT MACOM/DA STAFF OWNER INFORMATION.** See guidance at Section 3: "To Transfer a System".

c. **TO EDIT MISSION CRITICALITY INFORMATION**. Requests to change Mission Criticality will be coordinated with, and approved by, the Functional Proponent [the AITR POC from the Functional Proponent can provide this] prior to submission to the AITR Help Desk. Email your request for change to your MACOM/DA Staff AITR administrator for coordination with the Functional Proponent. The MACOM/DA Staff AITR administrator will email the coordinated response from the Functional Proponent to the AITR Help Desk for execution [aitr.help@us.army.mil]. Table 4 contains the list of Functional Proponents. Please provide the following information in your change Mission Criticality request:
   1) Owning MACOM: _____
   2) System Name: _____
   3) System Acronym: _____
   4) System AITR ID #: _____
   5) Primary Functional Area: _____
   6) Add the fact that you want to change Mission Criticality from [specify current criticality] to [specify desired criticality].

Table 4: Table of Functional Proponents

FUNCTIONAL AREAS	PROPONENT
Allies	G-3
Chemical, Biological, Radiological, and Nuclear and High Explosive (CBRNE)	G-3
Civilian Personnel & Readiness	ASA (M&RA)
Command and Control	G-3
Communications	CIO/G-6
Communications Security (COMSEC)	CIO/G-6
Economic	ASA (FM&C)
Environmental Security	ASA (I&E)
Facilities	ACSIM
Finance	ASA (FM&C)
Health/Medical	OSG/MEDCOM
Human Resources	ASA (M&RA)
Information Management	CIO/G-6
Inspector General	DAIG
Intelligence	G-2
Legal	OTJAG
Logistics	G-4
Military Personnel and Readiness	G-1
Nuclear	G-3
Nuclear, Chemical, Biological	G-3
Operations	G-3
Personnel and Readiness	G-1
Procurement/Acquisition	ASA (ALT)
Reserve Components	OCAR or DANG (depending on system ownership)
Scientific and Engineering	ASA (ALT)
Space and Weather	G-2
Test and Evaluation	DUSA-OR
Trainers	G-3
Transportation	G-4
Weapons	G-3
N/A	CIO/G-6

Note: the System Identification field and the DOD Registration Identification field are assigned by DA CIO/G6

d. **TO CHANGE PROJECTED WEBIFICATION DATES AND WEBIFICATION EXEMPTIONS**: System POCs and MACOM/DA POCs can enter initial Projected Webification dates into AITR themselves. Once the information has been initially entered, CIO/G-6 needs to be involved to *change* those dates. The following guidance is to be followed when requesting a webification information change. Paragraph 5 identifies the information required when submitting a Webification change request.

1) Remember, the SECARMY/CSA's guidance was to webify all systems. Waivers are not automatic. Your waiver request must still support the AKM vision, and make it very clear why this system should be exempt from the webification mandate.
2) Ongoing MACOM/DA Staff Sections must review the request and state whether their CIO/IMO supports the request. The AITR POC can provide this statement – we don't need anything directly from your SES/GO. However, CIO/G-6 expects the MACOM/DA Staff Section to review the request – not just forward all requests to CIO/G-6 for judgment. Many of the exemption requests we've received and rejected should have been caught at the MACOM/DA Staff level.
3) Each request for an exemption should be in a separate e-mail, so it may be routed to the appropriate staffers.
4) The title of the e-mail should read "Webification Exemption Request – (Insert System Acronym and AITR ID # Here)" or "Projected Webification Change Request - (Insert System Acronym and AITR ID # Here)" as appropriate. The email will be sent to the AITR Help Desk for execution [aitr.help@us.army.mil]; they will contact the appropriate CIO/G-6 approval authority.
5) The body of the e-mail should contain:
   a) Owning MACOM: _____
   b) System Name: _____
   c) System Acronym: _____
   d) System AITR ID #: _____
   e) Add the fact that you want a Webification Exemption or a Projected Webification Change.
   f) Add the Reason for the exemption or change in projected webification dates- this should be one or more of the following. Use these exact words:
      (1) System is being retired
      (2) System Processes Data at the Top Secret or Higher Level
      (3) System cannot be webified due to insurmountable technical challenges
      (4) System is a database that has no user interface – it merely collects data from other applications and databases and shares this data with other applications and databases.
      (5) System is not worth webifying from a cost/benefit standpoint
      (6) Other reasons (specify). Changes to projected dates fall in this category.
   g) Include MACOM Concurrence and Comments – state why your CIO/IMO concurs with the request

Table 5 provides additional information needed when submitting for Webification exemption, attach (at a minimum) the following:

Table 5: Addition information required when submitting for Webification Exemption

IF YOUR REASON FOR EXEMPTION IS:	THEN SUBMIT:
System is being retired	Name and AITR ID Number of system that will replace the retiring system (if replacing system is not Army Owned, list owning agency instead of the AITR ID Number. Include the date the system will be retired.

IF YOUR REASON FOR EXEMPTION IS:	THEN SUBMIT:
System processes data at the Top Secret or higher level	No additional data needed.
System cannot Be webified due to Insurmountable technical Challenges	Describe the challenges, and why your analysis proves them to be insurmountable.
System is a database that has no user interface – it merely collects data from other applications and databases and shares this data with other applications and databases.	Describe what the system does. List the systems (with AITR ID Numbers) that this system pulls data from or provides data to. If these are not Army systems, state the owner instead of the AITR ID Number.
System is not worth webifying from a cost/benefit standpoint	Submit the business case as to why webification is not justified. Remember, the waiver authority has no knowledge of your system, so make sure your business case is complete. If the issue is financial, include all the numbers that make your case.
Other Reasons (specify)	Provide all details necessary to make your case.

Note: Waivers will not normally be approved for the following reasons.

- "We don't want this data available to others outside our organization." Linking to AKO doesn't mean others can see your data. You can still protect it via passwords or any other form of security to ensure only authorized users can access it.

- "We don't have the funds." This is an Army directive. Your organization needs to program and budget the necessary funds. Since you set the date when your system will be webified, set it far enough in the future to give you time to get the funds you need.

- "This system is of no interest to anyone outside of our organization". There are benefits to webification even if the system will only be used by your own personnel. They will able to access the system from anywhere in the Army network using just a browser. You will no longer have to support administration of the client software. You will be able to add new users to your system without ever touching their desktop. If you can make a business case (with dollars) that the benefits of webification aren't worth the costs, provide the business case analysis as described above.

e. **TO CHANGE COMPLETED WEBIFICATION DATES OR TO REVISE WEBIFICATION EXEMPTIONS**. CIO/G6 needs to review these actions. Initiate your request by sending e-mail to your MACOM/DA Staff AITR Administrator. The MACOM/DA will forward email will to the AITR Help Desk for execution [aitr.help@us.army.mil] once they have coordinated. The following guidance is to be followed when requesting a change:
   1) Each request for a change should be in a separate e-mail, so it may be routed to the appropriate staffers.

2) The title of the e-mail should read "Completed Webification Change Request - (Insert System Acronym and AITR ID # Here)" or "Revision to Webification Exemption Request" as appropriate.
3) The body of the e-mail should contain:
   a) Owning MACOM: _____
   b) System Name: _____
   c) System Acronym: _____
   d) System AITR ID #: _____
   e) Add the fact that you want a Completed Webification Change or a Revision to Webification Exemption [i.e. a previously exempt system can now be webified] as appropriate.
   f) Add the Reason for change.
4) Include MACOM Concurrence and Comments – state why your CIO/IMO concurs with the request.

3. TO TRANSFER A SYSTEM: System records will be maintained by the owning organization. When the owner of an AITR system record determines another organization should own the record; send an e-mail in the format listed below to your MACOM POC. The MACOM POC will endorse your request and forward to the MACOM POC at the organization identified to gain the system record. The gaining organization will consider and respond to the request by e-mail to the requesting MACOM. Once concurrence is reached, the MACOM POC from the losing organization will email the AITR Help Desk with the concurrence. *What is ownership: There can only be one owner. If you fund, field and maintain it, it's yours. If it's a DoD system, it's not yours. If multiple organizations fund it, they must determine the "lead", who becomes the owner.*

a. The title of the e-mail should read "System Transfer Request – (Insert System Acronym and AITR ID # Here)"
b. The body of the e-mail should contain:
   1) Owning MACOM: _____
   2) System Name: _____
   3) System Acronym: _____
   4) System AITR ID #: _____
   5) Add the fact that you want to transfer the record

4. TO DELETE A SYSTEM: Systems should be deleted when they are no longer in use anywhere in the Army. Systems that are being transferred to another MACOM need to follow the transfer procedures in Section 3. Send an e-mail in the format listed below to your MACOM POC. The MACOM POC will endorse your request and forward to the AITR Help Desk who will submit to Army CIO/G-6 for approval. If approved, they will delete the system.

a. The title of the e-mail should read "System Deletion Request – (Insert System Acronym and AITR ID # Here)"
b. The body of the e-mail should contain:
   1) Owning MACOM: _____

2) System Name: _____
3) System Acronym: _____
4) System AITR ID #: _____
5) The Reason for the deletion - this should be one or more of the following. Use these exact words:
   a) System has been retired. The replacement system is (specify system name and, if an Army owned system, AITR ID#, and include the retirement date)
   b) System is a duplicate record (specify System Name, Owning MACOM, and AITR ID# of system that will remain in AITR).
   c) System is not owned by Army (specify name and point of contact of organization that owns the system)
   d) System does not meet definition of an information system (specify)
   e) Other reasons (specify)

5. TO DETERMINE WHAT IS IN THE DOD IT REGISTRY. MACOM and DA Staff level AITR administrators are provided access to a non public folder in the AKCC which is accessed under the hierarchy: "Army Communities," >"Army CIO/G-6," >"AKM," >"Goal 4," >"Strategic Partnering," >"MACOM System Reports," >"DOD IT Registry." This folder has a list of systems registered in the DOD IT Registry. You may also contact the AITR Help Desk [aitr.help@us.army.mil or 703-806-3507 or DSN 656-3507] with the name and acronym of a system and they will query the DOD IT Registry and provide you a report.

6. DEFINITIONS:

a. **Acquisition Program**. A directed, funded effort designed to provide a new, improved, or continuing materiel, weapon, or information system or service capability in response to a validated operational or business need. Acquisition programs are divided into different categories that are established to facilitate decentralized decision-making, execution, and compliance with statutory requirements. Technology projects are not acquisition programs. (DoDD 5000)

b. **Application**. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs. (DoDD 8500.1)

c. **Business Management Modernization Program (BMMP).** A plan to transform the Department of Defense's business processes. Formerly called the FMMP. The supporting architecture is Business Enterprise Architecture (BEA). Formerly the Financial Management Enterprise Architecture. This collaboration will greatly enable the transformation of DoD processes in coordination with the Domains. The architecture details improved business processes, standard data, and management information needs. The incorporation of accounting requirements and strong internal controls into the BEA will provide compliant financial reporting. http://www.dod.mil/comptroller/bmmp/pages/index.html

d. **DIACAP**. DoD Information Assurance Controls Verification and Authorization Policy (DIACAP) – The future replacement for the DITSCAP.

e. **DITSCAP**. DoD Information Technology Security Certification and Accreditation (C&A) Process. The DITSCAP certification and accreditation methodology replaces both AFSSI 5024 (Air Force) and AR 380-19 (Army).

f. **Embedded IT**. IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)
g. **Enclave.** Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. (DoDD 8500.1) Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.
h. **Exemption.** This IT system will never be web-enabled nor linked to AKO.
i. **Information System.** For the purposes of AITR, the terms "application" and "information system" are used synonymously - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. In other words, the application of IT to solve a business or operational (tactical) problem. System/Application owners will have to use judgment in how to report "systems of systems;" either as a single or separate entries. Standard COTS desktop office automation (i.e. word processors, spreadsheets, etc.) is exempt from the reporting requirements of this document.
j. **Integral to real-time execution**. IT which is integral to real-time execution of the platform mission (e.g., radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)
k. **Mission Assurance Category.** Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:
    1) **Mission Assurance Category I** (MAC I) - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
    2) **Mission Assurance Category II** (MAC II) - Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
    3) **Mission Assurance Category III** (MAC III) - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

l. **Mission Critical (MC) Information System.** An information system that meets the definition of "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of war fighter operations or direct mission support of war fighter operations.
m. **Mission Criticality.** Every IT system within AITR needs to be classified as Mission Critical, Mission Essential, or "Other."
n. **Mission Essential (ME) Information System.** An information system that is basic and necessary for the accomplishment of one or more of the Army's missions.
o. **National Security Systems (NSS).** Any telecommunications or information system operated by the Department of Defense, the function, operation, or use of which 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapons system; or 5. is critical to the direct fulfillment of military or intelligence missions, but does not include a system, and equipment and services of a system, that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications) (Source: Title 10. USC, Section 2315).
p. **Network**. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan or wide area and backbone networks. (DoDD 8500.1)
q. **"Other" Information System.** An information system that does not meet the definitions of Mission Essential or Mission Critical.
r. **Ownership.** There can only be one owner. If you fund, field and maintain a system, it's yours. If it's a DoD system, it's not yours. If multiple organizations fund it, they must determine the "lead", who becomes the owner.
s. **Privacy Impact Assessment (PIA)**. An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment for a new or previously existing IT system based on the provisions in OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIB. http://www.whitehouse.gov/omb/memoranda/m03-22.html
t. **System.** Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (DoDD 8500.1)
u. **Systems Security Authorization Agreement.** The phases of the SSAA are based on Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) definitions:
    1) **Phase I** - The Definition Phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority (DAA) and Certification Authority (Certifier), and document the C&A security requirements. Phase 1 culminates with a documented

agreement between the Program Manager, DAA, Certifier, and user representative on the approach and results of the Phase 1 activities.

2) **Phase II** - The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (h)), there is a corresponding set of security activities that verifies compliance with the security requirements and constraints and evaluates vulnerabilities.
3) **Phase III** - The Validation Phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. Validation culminates in an approval to operate.
4) **Phase IV** - The Post Accreditation Phase includes activities to monitor system management, configuration, and changes to the operational and threat environment to ensure an acceptable level of residual risk is preserved. Security management, configuration management, and periodic compliance validation reviews are conducted. Changes to the system environment or operations may warrant beginning a new DITSCAP cycle.

v. **Webification.** For the purposes of Goal 4, a Webified system is both:
1) **Web Enabled.** System runs on a JTA-Army -approved browser without the need to preload any other software onto the client prior to first web access (software may be downloaded as part of the login).
2) **AKO-Linked.** System is web enabled and linked through a page on AKO or AKO-S so that users can get to the system via the portal.

w. **Waiver.** For the purpose of Goal 4, a system that has a waiver if it has an approved future webification date or a CIO/G6 approved exemption.

x. **Without Platform Interconnection**. IT which does not communicate outside the platform

7. VERSION:

Version	Description	Date
Initial draft	**First consolidated policy guidance**	**06 November 2003**
Second draft	**Updates guidance to reflect addition of new fields for Federal Information Security Management Act (FISMA) and Business Management Modernization Program (BMMP)**	**18 December 2003**
Third draft	**Updates guidance to reflect addition of new fields for Privacy Impact Assessment (PIA)**	**23 February 2004**
Current version	**Changes functional proponent for "Command and Control" systems to G-3, minor editorial fixes, adds Version section**	**09 April 2004**